Translation

Japanese Patent Application Public-disclosure No. 10-93547
Japanese Patent Application Public-disclosure date: April 10, 1998
Title of the invention: Communication equipment, system and method
Japanese Patent Application No. 8-243181
Japanese Patent Application date: September 13, 1996
Applicant: Canon Inc.
Inventor: Keiichi Iwamura

[Claims]

1. Communication equipment for conducting encryption/authentication communications of a layered construct in which a key belonging to a higher layer converts a key or data belonging to a lower layer,

said equipment being provided with a means for setting communication quality such that quality of said encryption/authentication communications concerning a higher layer is higher than that concerning a lower layer.

2. The communication equipment as defined in Claim 1 further provided with a means for optionally setting communication quality for each layer.

3. A communication system comprising the communication equipment set forth in Claim 1 or 2.

4. A communication system wherein quality of communication in Claim 1, 2 or 3 is a parameter defined as a QOS in ATM communications.

5. A communication method for conducting encryption/authentication communications of a layered construct in which a key belonging to a higher layer converts a key or data belonging to a lower layer,

said method being provided with a means for setting communication quality such that quality of said encryption/authentication communications concerning a higher layer is higher than that concerning a lower layer.

[Detailed explanation of the invention]

The present invention pertains to communication equipment, system and method for transmitting information such as moving picture data, still picture data, voice data, computer data, etc. in a multimedia network.

[Prior art]

A B-ISDN (Broadband-Integrated Services Digital Network), which is expected to constitute a main communication infrastructure in the next generation, is a flexible network having a greater transmission capacity than existing ISDN and having capabilities of providing communication service of a requested transmission capacity (within a permissible range of a network resource). A B-ISDN attributes its successful

delivery of such advanced services solely to the technology called ATM (Asynchronous Transfer Mode). In ATM networks, as in packet switching transmission mode networks, cells of a fixed length respectively provided with a header storing a label on which a destination is written are transmitted to handle an optional speed and upon reading the label, a switching facility conducts switching. Since a packet consists of cells of a fixed length, high-speed synchronous communication can be conducted at a physical layer level and an optional transfer speed can be secured according to packet transmission density.

In order to guarantee secure use of such a communication infrastructure, network security technology such as encryption, authentication, etc. is vital. As is publicly known, encryption and authentication can be performed by a common key cryptosystem wherein the same enciphering key is secretly shared by the sender and the recipient (, which is also referred to as a secret key cryptosystem, symmetric cryptosystem, conventional cryptosystem, etc.) or a public key cryptosystem wherein one key, usually the enciphering key, is made public and a different key, usually the deciphering key, is kept secret (as for the details of the respective cryptosystems, see "Contemporary cryptography" co-written by Ikeno and Koyama and published by the Electronic Information Communication Congress in 1986). Further, various systems for securely distributing such keys have been proposed (see, for example, "Encryption and information security" co-written by Tsujii and Kasahara and published by Shokodo in 1990). By utilizing the aforementioned techniques, secure data communications in the B-ISDN can be realized.

[Problems to be solved by the invention]

With a view to enhancing security in encryption/authentication communication such as described above, normally, hierarchically arranged keys as indicated in Fig. 6 are employed. However, since all data can be decrypted once an enciphering key is decoded, security needs be enhanced by, for example, enciphering a key by means of another key belonging to a higher layer or employing a plurality of keys for varying usage (for example, a signature key and an enciphering key) to simultaneously perform an encryption function and an authentication function. In this case, the encryption function may be replaced with a deciphering function, signature function, verification function, etc.

In Fig. 6, a first key for key encryption is referred to as a master key and a key for directly enciphering data is referred to as a work key and the other keys are referred to as key encryption keys. Some of the key encryption keys including the master key are either distributed to users in advance or public keys accessible by anyone. In the meantime, some of the key encryption keys including the work key are either keys set for temporary usage by the sender, recipient or organization, etc. in charge of the keys or keys to be sent together with data in order to save time for retrieving keys or identifying the sender.

Such keys are usually sent to the recipient together with and/or separately from enciphered data or data prefixed with signature. Thus, encryption/authentication communication involves not only data communication but also key communication, and it should be obvious that security of the communication concerning keys of higher layers of the hierarchy in Fig. 6 is more important than that concerning keys of lower layers,

because if communication concerning a higher layer of the hierarchy is not reliable, communication concerning any layers lower than that can hardly be considered to be reliable. However, in conventional communications, key information and data information concerning the higher layers is not distinguished from that concerning the lower layers; or even if they are differentiated according to location of information, etc., none of the conventional communication systems proposes differentiation of information according on the basis of its significance.

[Means for solving the problems]

The present invention has been accomplished with a view to obviating the aforementioned problems of the prior art and provides communication equipment, system and method capable of conducting communications by utilizing information such as significance of data, service, etc. to be transmitted.

In order to achieve the aforementioned object, the present invention pertains to an encryption/authentication communication system for conducting encryption/authentication communications of a layered construct where a key belonging to a higher layer converts a key or data belonging to a lower layer to effectuate communications, said system being provided with a means for setting communication quality such that quality of said encryption/authentication communications concerning a higher layer is higher than that concerning a lower layer.

[Embodiment 1]

Hereafter, an embodiment of the present invention will be specifically explained with reference to the attached drawings.

Since multimedia communication is conducted in a B-ISDN, the present embodiment allows different media to have different traffic characteristics. Therefore, different media require different QOS (Qualities of Service). In the case of ATM, cell transfer delay, cell delay variation, cell loss rate (CLR), etc. are defined as QOS parameters (further study is required for other parameters).

"Delay" in this context means time that elapses between the instant at which data is transmitted and the instant at which the data is received, and "delay variation" means dispersion in cell transfer time due to congestion, etc. Since delay variation in image transmission causes fluctuation of the number of bits received during a certain period of time, it results in flicker on the screen unless the recipient side has sufficient buffer memory. Further, when delay becomes substantial in the case of transmission of conversational voice data, etc., an echo cancellation problem must be solved. On the contrary, when data to be transmitted is text data, etc., neither delay nor delay variation causes problems. Still further, cell loss rate (CLR) represents the ratio of the number of dropped cells divided by the total number of cells received. Thus, if CLR is high in the case of image transmission where data is continuously transmitted without checking their safe arrival at the recipient, a frame drops or noise arises and therefore, CLR affects communication quality substantially. It should be obvious that in data compression performed based on predictive coding such as MPEG, high CLR could lead to even more serious deterioration of image quality. Thus, each QOS parameter has different requested requirements according to usage.

Between a user and the network, QOS requirements are set up as follows. A user requests a QOS class from a plurality of QOS classes provided by the network (a QOS

class consisting of a combination of several QOS parameters) normally when a connection is set up and a traffic contract is entered. At this time, the network determines whether the requested traffic does not exceed actual transmission capacity and also whether the requested QOS class can be secured, and if the network decides that the communication is viable, it informs a terminal accordingly and enters a communication mode. In the communication mode, the network maintains the requested QOS and guarantees the requested quality as long as the user observes the traffic contract.

Further, various protocols (communication protocol) are specified for communications and a B-ISDN protocol is hierarchized as is indicated in Fig. 7 so that addition or change of various functions does not affect the whole. There is a specified data transmission agreement between layers. In Fig. 7, the physical layer corresponds to a protocol concerning physical media (specifications of a cable and connector, construction of a transmission frame, cell insertion, extract function, etc.) and the ATM layer corresponds to a protocol for handling multiplexing and exchange of cells common to all service. The asynchronous transfer mode adaptation layer (AAL) corresponds to a protocol for handling functions dependent on each service and has a plurality of protocols set corresponding to each service. The AAL absorbs addition and change of functions of the high layer dependent on each service so that it does not affect the basic functions of a B-ISDN system. Therefore, conversion of QOS requested by each service to QOS of the aforementioned ATM and reverse-conversion of the same is conducted at high layers including the AAL

Thus, in a B-ISDN system, quality of communications can be designated by means of QOS.

Therefore, the present embodiment is provided with a means for setting significance (quality) of QOS in accordance with the hierarchy shown in Fig. 6, i.e., a means for setting higher quality QOS in terms of cell loss rate, etc. for communications concerning higher layers than for communications concerning lower layers, whereby communications commensurate with significance of information of encryption / authentication communications can be realized.

Fig. 1 is a flow chart describing an operation of the embodiment of the present invention. In the drawing, an example of a means for setting up a connection having QOS according to a layer comprises a QOS setting means for requesting/setting QOS and a QOS memory means for receiving information about a layer and storing a table of QOS corresponding to the layer. A control means such as a CPU, etc. controls the entire operation indicated in the flow chart of Fig. 1, including an operation for outputting information about a layer. Layer information K in Fig. 1 represents the total number of layers in the hierarchy in Fig. 6 and therefore, the highest layer is K, the second highest layer being K – 1 and so on. Thus, when a communication request occurs, the means shown in Fig. 1 requests and sets up a highest QOS on the assumption that the layer information is K. Using the thus established connection, the means conducts key encryption and authentication communications by means of the master key of the highest layer. Upon completion of the above key encryption and authentication communication, the means shown in Fig. 1 closes the connection. Then, the means decrements the layer information K by 1 and requests and sets up QOS corresponding to the decremented layer information. The means repeats the aforementioned operation until K becomes equal to 0. When there is a key that does not require the same communication as the master key

requires, however, processing for opening/closing connection as well as encryption/authentication communication is omitted.

On the other hand, when there are no keys other than the master key that do not require communications, processing for determining if key communications is necessary is omitted. Further, if a few layers correspond to the same QOS, processing for opening/closing connection does not have to be repeated for each of the layers. Such a change in control as mentioned above can be easily made by changing programming of the control means. Further, the present invention can be implemented without the QOS memory means if QOS for each layer is programmed in advance. Still further, QOS need not rigidly be set for each layer and the present invention may be implemented by performing processing such as requesting the highest available QOS in the event of communications concerning the highest layer. Still further, QOS for communications concerning higher layers need not be of higher quality than those for communications concerning lower layers and may be set differently depending on how to set the QOS memory means or how to program the QOS setting means. Since a series of communications (spanning a plurality of connections) indicated in Fig. 1 are all related to one another, identifiers, etc. can be employed to differentiate communications from one another.

The above is effective for connection-type communications wherein QOS is set at the stage for setting up communications.

[Embodiment 2]

A B-ISDN system provides not only various QOS but also various connection setting modes such as a connection mode wherein a connection is established prior to transmission of information, a connectionless mode wherein when send information occurs, a connection is established to transmit the information, etc. The aforementioned embodiment 1 pertains to a connection mode communication service. The embodiment 2 pertains to connectionless mode communication service wherein QOS can be changed in the midst of communications.

Fig. 8 shows an example of a configuration of protocols for connectionless mode communication service. In the drawing, a CLNAP (Connectionless Network Access Protocol) layer is a part of the high layer shown in Fig. 7, where protocols for the connectionless mode communication service are implemented. Fig. 9 shows a format of a PDU (Protocol Data Unit) at the CLNAP layer. PDU represents a set of data designated in protocols at a specified layer whereas SDU represents a set of data transmitted by users of services at a specified layer. In this case, QOS is designated as 4-bit data in the header of PDU, which is generated in the CLNAP layer. PDU is turned into cells or synthesized at the AAL and ATM layers and transmitted via the physical layer. Therefore, in the connectionless mode communication service, QOS can be set for each PDU.

Thus, according to the connectionless mode communication service protocol, different PDUs are generated at different layers (for different QOSs) and QOS corresponding to a layer of encrypted information contained in the PDU is set, whereby communications commensurate with significance of information (layer) can be realized.

Such connectionless mode communications can be implemented by replacing "connection" in Fig. 1 with "PDU".

Fig. 3 is a conceptual diagram of the embodiment 2 of the present invention. The encryption means shown in Fig. 3 receives input data, encrypts the data and transmits the thus encrypted information to the QOS setting means and further transmits the layer information to the QOS memory means. It is assumed that a key for each user such as a master key, etc. is managed by a known key management means. If not (if, for example, a key is input through an external card, etc.), the key is input to the encryption means via communications, etc. In the meantime, a temporary key such as a work key, etc. is generated by using a known random number generator, operation means, etc. Further, encryption by means of the keys is conducted by a known encryption processing means and encrypted information output from the encryption processing means is sent to the QOS setting means. Since the order of use of the keys is determined in advance in such a manner as to correspond to the hierarchy of the keys, the control means provides to the encryption processing means a master key, etc. from the key management means (or external card, etc.) and a work key, etc. from the random number generator and operation means, etc. in compliance with the prescribed order of use of the keys, causes the encryption processing means to encrypt input data by using the keys (a work key, etc. may constitute data) and sends to the QOS memory means the order of the processing as layer information.

The QOS memory means, which comprises a memory means for storing QOS corresponding to layer information in a table, provides the QOS setting means with QOS corresponding to the layer information input from the encryption means. The QOS setting means sets and outputs the QOS at a predetermined location and/or in a predetermined format as output data (predetermined information including the encrypted information).

Next, the embodiment 2 with respect to the recipient side will be explained with reference to Fig. 4.

It is assumed here that the recipient receives communications conducted by the means shown in Fig. 1. In Fig. 4, the QOS analysis means resolves the input data into the encrypted information and the layer information based on the location of prescribed information and format of an identification signal, etc. and sends them to the decoding means. If it transpires that the layer information concerns a layer managed by the key management means, the control means in the decoding means retrieves the key from the key management means, inputs the key to the decoding processing means and decodes the encrypted information. Further, if it transpires that the result of the decoding corresponds to information about a layer used as a key, the result of the decoding is temporarily stored in the key memory means. On the contrary, if it transpires that the layer information concerns a layer not managed by the key management means, the control means retrieves information constituting a key of the layer from the stored result of the decoding and inputs the retrieved information as a key to the decoding processing means, which decodes the encrypted information and outputs the thus decoded information. However, a key may be generated by the operation means based on the result of the decoding. Therefore, it is obvious that the QOS analysis means can be implemented by combining a processing means such as a CPU, DSP, etc. with a memory means such as RAM, etc., whereas the decoding processing means may be a known

decoding processing means corresponding to the encryption processing means in the embodiment 1 and the key management means may be a means similar to that of the embodiment 1 and the control means may be a processing means such as a CPU, DSP, etc. and further, the operation means may be a CPU, DSP, etc.

Although the above explanation concerns encryption and decryption, encryption and decryption may be replaced by signature and verification respectively if authentication communications is also involved, whereby authentication communications commensurate with significance of keys can be implemented by employing the same means as in the case of encryption communications. Further, in the case of a system for conducting both sending and receiving, the means shown in Figs. 3 and 4 may be synthesized to prepare a means (program) since the components in Figs. 3 and 4 are similar.

[Embodiment 3]

The embodiments 1 and 2 represent means for implementing communications commensurate with significance of information in connection mode communication service and connectionless mode communication service respectively. In the present embodiment 3, a communication system including the embodiments 1 and 2 for implementing communications commensurate with significance of information will be specifically explained with reference to Fig. 5

It is assumed here that the means of the embodiment 1 are incorporated in the sender's terminal and/or the recipient's terminal in Fig. 5 and the number of layers K is 2 in the hierarchy of Fig. 6, i.e., there are only a master key and a work key. Further, a case where in the connection mode communication service, encryption and authentication processing concerning keys and data is performed according to the following ID-based key sharing system, will be explained below.

[ID-based key sharing system]

There is a center for managing the key distribution means. The center receives an identifier (ID) such as a name, telephone number, etc. of each entity, generates a secret key corresponding to the ID by using a secret algorithm inherent to the center and sends the thus generated secret key to each entity, whereby each entity calculates from the secret key and published ID of the other party of its communications an encryption key to be shared by the entity and the other party. This system is referred to as an ID-based key sharing system, according to which identification of a communication party and key sharing can be simultaneously conducted.

The ID-based key sharing system can be divided into two systems, that is, a system that requires spare communications prior to encryption communications and a system that does not require spare communications. The system that requires spare communications cannot be used like an e-mail system, etc. where only messages are encrypted to be transmitted. On the other hand, a system that does not require spare communications can be used like an e-mail system and therefore is more extensibly applicable. However, if many entities conspire in the system that does not require spare communications, the center's secret could be divulged. As a system that requires spare communications, a key distribution system by Okamoto (Sakae) is known well, whereas

as a system that does not require spare communications, a key distribution system by Matsumoto and Imai is well known (as for the details of the system, see Chapter 4 of "Encryption and information security" co-authored by Tsujii and Kasahara, published by Shokodo in 1990). Hereafter, the key distribution system by Okamoto (Sakae) will be explained as an example of a system that requires spare communications.

<Key distribution system by Okamoto (Sakae)>

1) A center makes RSA encryption public, which is one of the public key cryptosystems, as a unidirectional function. In other words, two prime numbers p and q and a decoding key d are kept secret whereas n = (p · q) and the encryption key e (e · d =1 mod (p – 1) · (q – 1)) are made public. A source element g of the finite fields GF (p) and GF (q) is also made public.

2) At the time of subscription to a network, each user j registers his (her) own identifier IDj at the center and the center calculates and sends Sj = IDjd mod n to the user j. The user j keeps Sj = IDjd mod n secret.

3) When user A and user B share a key, the following communications and calculations i ~ iv are conducted.

i. The user A arbitrarily chooses random number kA and sends CA = SA · gkA mod n to the user B.

ii. The user B arbitrarily chooses random number kB and sends CB = SB · gkB mod n to the user A.

iii. The user B calculates y = (CAe/IDA) kB mod n (= ge · kA · kB mod n).

iv. The user A calculates y = (CBe/IDB) kA mod n (= ge · kA · kB mod n).

4) The users A and B conduct encryption communications, using y as a shared key.

A master key corresponds to Sj in 2) and a work key corresponds to y in 3). Thus, Sj in 2) is distributed in advance to each user and the processing/communications in 3) corresponds to encryption/authentication communications concerning a key whereas the communication in 4) corresponds to encryption communications conceming data. Further, the user A and the user B correspond to the sender and the recipient in Fig. 5 respectively. In the following explanation, it is assumed that each terminal in Fig. 5 comprises a known ID-based key sharing means in addition to the means of the embodiment 1 (the aforementioned Sj is normally managed by the ID-based key sharing means).

First, when the user A conducts encryption/authentication communications with the user B, the user A first negotiates with the network over QOS by means of the embodiment 1 on the assumption that K is 2 and establishes a connection of a high quality QOS with the user B. Upon setting up the connection, the user A performs the processing/communications set forth in 3) with the user B by using the known ID-based key sharing means, whereby the user A and the user B share their respective work key y and temporarily terminate the connection. Subsequently, the user A negotiates again with the network over QOS on the assumption that this time, K is 1 and establishes a connection with the user B, which connection has QOS lower than the QOS for K being 2. Using the thus established connection, the user A conducts encryption communications with the user B by means of the work key y.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－93547

(43)公開日　平成10年(1998)４月10日

(51)Int.Cl.⁶		識別記号	FI		
H04L	9/14		H04L	9/00	641
	9/08				601Z
	9/32				675A
// H04L	12/28			11/20	D

審査請求　未請求　請求項の数５　ＯＬ　（全８頁）

(21)出願番号　特願平8－243181

(22)出願日　平成８年(1996)９月13日

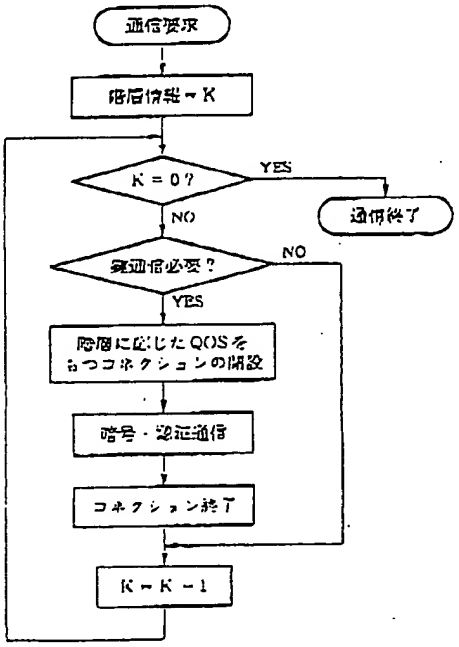
(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

(74)代理人　弁理士　大塚　康徳　（外１名）

(54)【発明の名称】　通信装置及びシステム及び方法

(57)【要約】
【課題】　情報やサービスの重要度といった特徴を生かす通信を可能にする。
【解決手段】　階層的に構成され、上位階層に属する鍵が下位階層に属する鍵またはデータを変換して通信を行う暗号・認証による通信を行う場合に、上位階層に関する該暗号・認証通信の品質がそれより下位の階層に関する該暗号・認証通信の品質より高くする。



【特許請求の範囲】
【請求項1】 階層的に構成され、上位階層に属する鍵が下位階層に属する鍵またはデータを変換して通信を行う暗号・認証による通信通信であって、
上位階層に関する該暗号・認証通信の品質がそれより下位の階層に関する該暗号・認証通信の品質より高くなるように、通信の品質を定める手段を有することを特徴とする通信装置。
【請求項2】 更に、各階層毎の通信品質を任意に定める手段を有することを特徴とした請求項第1項に記載の通信装置。
【請求項3】 請求項1或いは請求項2のいずれかの通信装置によって構成されることを特徴とした通信システム。
【請求項4】 請求項1ないし請求項3のいずれかの通信の品質をATM通信におけるQOSとして定義されるパラメータとすることを特徴とした通信システム。
【請求項5】 階層的に構成され、上位階層に属する鍵が下位階層に属する鍵またはデータを変換して通信を行う暗号・認証による通信方法であって、
上位階層に関する該暗号・認証通信の品質がそれより下位の階層に関する該暗号・認証通信の品質より高くなるように、通信の品質を定める手段を有することを特徴とする通信方法。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、動画像データ、静止画像データ、音声データ、コンピュータデータ等の情報を伝送するマルチメディアネットワークにおける通信装置、システムおよび方法に関するものである。
【0002】
【従来の技術】次世代の基幹系通信インフラとして検討されているB-ISDN（BroadbandAspects of Integrated Services Digital Network：広帯域サービス総合ディジクル網）は、現在施行されているISDNに比べ、伝送容量が大きく、かつ、（ネットワーク資源の許す限り）要求された伝送容量で通信サービスを提供することができる、柔軟なネットワークである。この様なサービスが可能なのは、一重にATM（Asynchronous Transfer Mode：非同期転送モード）と呼ばれる、B-ISDNの基幹技術によるものである。ATMでは、パケット交換伝送モードと同様に、宛先の書かれたラベルを格納したヘッダを付与した固定長のセルを送出することで任意速度に対応し、そのラベルを読むことで、交換機がスイッチングする、パケットが、固定長のセルという単位で構成されることで、物理層レベルでは高速同期通信が行え、パケット送出密度により任意の転送速度を確保できる。
【0003】一方、このような通信インフラをユーザが安心して使えるためには、暗号・認証等のネットワークセキュリティ技術を必要とする。この暗号や認証は送信者と受信者で同一の暗号鍵を秘密に共有する共通鍵暗号方式（秘密鍵暗号方式、対称暗号方式、慣用暗号方式とも呼ばれる）や、暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する公開鍵暗号方式によって実現できることが知られている（各暗号方式の詳細は池野，小山著「現代暗号理論」電子情報通信学会、1986．参照）．また、この様な鍵を安全に配送する方式に対しても種々の鍵配送方式が提案されている（たとえば辻井，笠原著「暗号と情報セキュリティ」昭晃堂，1990．参照）．以上のような技術を用いることによって、B-ISDNに対しても安全な通信を実現することができる。
【0004】
【発明が解決しようとする課題】上述のような暗号・認証通信においてはその安全性を高めるために図6に示すように鍵を階層化して用いる場合が多い。これは、鍵が解析されれば以後のデータは全て解読されてしまうために、鍵をさらに上位階層の鍵で暗号化することによって安全性を高めたり、用途の異なる鍵（署名用の鍵と暗号用の鍵等）を複数用いることによって、暗号と認証の機能を同時に実現する等のために行われるものである。この場合、暗号化を復号、署名、検証と用途に応じて置き換えれば種々の機能に対応する。
【0005】図において鍵暗号化の最初となる鍵をマスタ鍵、直接データを暗号化する鍵をワーク鍵と呼び、それ以外の鍵は鍵暗号化鍵と呼ぶ。マスタ鍵を初めとする幾つかの鍵暗号化鍵は予めユーザに配送されている鍵であったり、誰でもがアクセスできる公開の鍵であったりする。また、ワーク鍵を初めとする幾つかの鍵暗号化鍵は送信者、受信者または鍵を管理するセンタ等がその場限りに設定した鍵であったり、鍵検索の手間を省いたり、送信者を特定するためにデータと共に送られる鍵であったりする。
【0006】このような鍵は暗号化または署名したデータと共にかつ／または別に受信者に送られることが多い。よって、暗号・認証通信にはデータに関する通信の他に鍵に関する通信が存在する．そして、その通信に関する安全性は図6の上位の階層に関する通信の方がより重要であることは明らかである。なぜならば、上位の階層に関する通信が信頼できなければそれ以下の階層に関する通信は全て信頼できないためである。しかしながら、従来の通信において上位階層や下位階層に関する鍵情報とデータ情報を区別していなかったり、情報の位置等によって区別していても、情報の重要度という意味で区別して通信する方式は提案されていなかった。
【0007】
【課題を解決するための手段】本発明は上述のような実情に鑑みてなされたものであり、情報やサービスの重要度といった特徴を生かすことのできる通信装置およびシ

ステムおよび方法を提供しようとするものである。

【0008】この課題を解決するため、たとえば本発明の通信装置は以下に示す構成を備える。

【0009】階層的に構成され、上位階層に属する鍵が下位階層に属する鍵またはデータを変換して通信を行う暗号・認証による通信通信であって、上位階層に関する該暗号・認証通信の品質がそれより下位の階層に関する該暗号・認証通信の品質より高くなるように、通信の品質を定める手段を有することを特徴とする。

【0010】

【発明の実施の形態】以下、添付図面に従って本発明に係る実施形態の一例を詳細に説明する。

【0011】先ず、本実施形態では、B-ISDNにおいてはマルチメディアを扱うために各メディアで異なるトラフィック特性を許容する。そのために、メディア毎に異なるQOS（Quality Of Service：サービス品質）が要求される。ATMにおけるQOSとしては遅延と遅延変動の感度、セルの損失率等が一式のパラメータとして定義されている（他のQOSパラメータについては今後の検討課題）。

【0012】ここで、遅延とはデータが発信されてから受信されるまでの時間であり、遅延変動は輻輳などによるセルの転送時間のバラツキである。映像伝送の場合、遅延変動はビットのゆらぎを引き起こすための受信側で十分なバッファメモリを持ってなければ画面がちらつくことになる。また、遅延が大きくなると会話用音声データのようにリアルタイム性が必要なものについては、エコーキャンセルなどの工夫が必要となる。逆にリアルタイム性の少ないテキストデータであれば、遅延は遅延変動と共に全く問題はない。セル損失率は、発信者により送出されるセルの総数と着信者に届かないセルの総数の比率を定義するものであり、データを垂れ流すタイプの映像伝送においては、フレーム落ちが起こったり、ノイズが出たりするので通信品質への影響は大きい。また、最近研究の進んでいるMPEG等の予測符号化を基本とする圧縮方式では、さらに大きな画質劣化を引き起こし得るのは理解できよう。このように、QOSの各パラメータは用途によってその要求が異なる。

【0013】ユーザとネットワーク間でのQOSの要求・設定は次のように行われる。ユーザはネットワークが提供するQOSクラス（幾つかのQOSパラメータを組み合わせたもの）の中から、あるクラスのQOSを要求する。これはトラフィック契約等とともに通常は通信の設定段階（可能な場合は通信途中でも再設定）で行われる。この時、ネットワークは要求されたトラフィックが実際の伝送容量を超えないかの判断をすると同時に要求されたQOSクラスが確保できるか等を判断して、通信可能ならば端末に通知し通信モードに入る。通信モードにおいて、ユーザがトラフィック契約を遵守している限り、ネットワークは要求されたQOSを維持し、要求された品質を保証する。

【0014】また、通信においては種々のプロトコル（通信規約）が定められ、B-ISDNのプロトコルでは、いろいろの機能の追加や変更が全体に影響を及ぼさないように、図7に示すようなプロトコルの階層化が行われている。各階層間では受け渡しの約束が決められており、個々の階層をレイヤと呼ぶ。図7において、物理レイヤは文字通り物理媒体に関する規定（ケーブル、コネクタの仕様の他に伝送フレームの構成、セル挿入、抽出機能を含む）であり、ATMレイヤは全てのサービスに共通なセルの多重化及び交換を行う。AAL（ALTアダプション・レイヤ）は各サービスに依存する機能を扱い、各サービスに対応して複数のプロトコルが規定されている。このAALによって、各サービスに依存する上位レイヤの機能の追加、変更を吸収し、B-ISDNの基本機能に影響を与えないようにしている。よって、各サービスが要求するQOSの上述のATMのQOSへの変換、及び逆変換は、AALを含む上位レイヤで行われる。

【0015】このように、B-ISDNにおいてはQOSを用いて通信の品質を指定することができる。

【0016】よって、本実施形態では、このQOSに図6の階層に応じた重要度（品質）を設定する、即ち、セル損失率等において上位階層に関する通信はそれ以下の階層に関する通信以上のQOSの品質を設定する手段を有することによって暗号・認証通信の情報の重要度に応じた通信を実現するものである。

【0017】図1に本発明の実施形態に対するフローチャートを示す。図において、階層に応じたQOSをもつコネクションの開設を実現する手段として一例として図2に示すような前記のQOS要求・設定手順を行うQOS設定手段と、階層情報を受けそれに対応するQOSをテーブルとして格納したQOS記憶手段によって構成できる。また、図1のフローチャートの全体の制御、及びその一部としての階層情報の出力はCPU等の制御手段によって行われる。ただし、図中の階層情報Kは図6の階層の総数に当り、最上位層をKとし下位階層になるにつれて小さくなるとする。よって、通信要求が生じた時、図1の手段はまず階層情報をKとして最も高品位のQOSを要求・設定する。そのコネクションを用いて最上位のマスタ鍵による鍵暗号化鍵の暗号・認証通信を行う。図1の手段は該暗号・認証通信終了後コネクションを閉じる。その後、階層情報Kを1ずつ小さくして、その階層に応じたコネクションを再び要求・設定して前記の動作を繰り返し、K＝0となれば終了する。ただし、鍵の中にマスタ鍵と同様の通信を必要としない鍵がある場合は、コネクション開閉処理と暗号・認証通信は省略される。

【0018】また、マスタ鍵以外に通信を必要としない鍵がない場合は鍵通信の必要性を判定する処理は省略さ

れる。また、幾つかの階層に亙ってQOSが同じである場合は、コネクションの開閉に関する処理を階層毎に行う必要はない。これらの制御の変更は制御手段へのプログラミングの変更等によって容易に可能である。さらに、QOS記憶手段がなくても階層に応じたQOSを予めプログラミングしておく等によっても本発明は実現できる。また、階層に対して固定のQOSでなくても、上位階層の場合にはその時点で要求できる最高のQOSを要求する等の処理をしても良い。また、QOSは上位階層が下位階層に対して必ず高品位でなくても、QOS記憶手段の設定やQOS設定手段のプログラミング等によって任意に設定することができる。ただし、図1の一連の通信（複数のコネクションにまたがる）は関連しているので、通信には他の通信を区別するために識別子のようなものを用いることができる。

【0019】以上は、通信の設定段階でQOSを定めるコネクション型の通信に対して有効である。

【0020】<第2の実施形態>B-ISDNでは種々のQOSの他に、情報の転送に先立って通信を設定するコネクション型と、送信情報が発生した時点で相手に情報を通信するコネクションレス型などの様々なコネクション設定形態も提供している。前述の実施形態（第1の実施形態）はコネクション型の通信に対するものであった。本第2の実施形態では、通信途中でQOSを変更できるコネクションレス型に対する場合を示す。

【0021】図8にコネクションレス型のプロトコルの構成の一例を示す。図において、CLNAP(Connectionless Network Access Protocol)は図7に示される上位レイヤの一部であり、コネクションレス型のプロトコルを実現するレイヤである。そのレイヤにおけるPDU(Protocol Data Unit)フォーマットは図9のように示される。PDUとはプロトコルを規定するデータ単位を示すものであり、SUD(Service Data Unit)は、プロトコルを使用するユーザからのデータ単位である。この場合、QOSはPDUのヘッダ中の4ビットのデータとして指定され、このPDUはCLNAPレイヤにおいて生成される。このPDUをAAL、及びATMレイヤにおいてセル化または合成され、物理レイヤを介して送信される。よって、コネクションレス型ではPDU毎にQOSを設定することができる。

【0022】よって、コネクションレス型の通信プロトコルでは、階層毎（異なるQOS毎）に異なるPDUを発生させ、そのPDUに含まれる暗号情報の階層に応じてQOSを設定することによって、情報の重要度（階層）に応じた通信を実現する。これは図1のコネクションをPDUに置き換えた制御によって実現できる。

【0023】図5に本第2の実施形態における構成概念図を示す。図示に示す暗号化手段は入力データを受けてそれを暗号化した情報をQOS設定手段に、階層情報をQOS記憶手段に送る。ただし、マスタ鍵等のユーザ毎の鍵は公知の鍵管理手段によって管理されているとするが、そうでない場合（外部のカード等から鍵を入力する場合など）、鍵は通信等を介して暗号化手段に入力される。また、ワーク鍵等のその場限りの鍵は公知の乱数生成手段や演算手段等を用いて生成される。また、それらの鍵による暗号化は公知の暗号処理手段によって実現され、出力される暗号情報はQOS設定手段に送られる。さらに、それらの鍵の使用順序は予め定められており、その使用順序が鍵の階層に相当するので、制御手段は予め定められた鍵の使用順序（階層）に基づき、前記鍵管理手段（または外部）からマスタ鍵等や前記乱数生成手段及び演算手段からワーク鍵等を前記暗号処理手段に与え、それに対応したデータの入力（ワーク鍵等がデータとなる場合もある）に応じて暗号化を行わせ、その処理順序を階層情報としてQOS記憶手段に送る。

【0024】次に、QOS記憶手段は階層情報に対応するQOSをテーブルとして記憶する記憶手段によって構成され、入力された階層情報に応じたQOSをQOS設定手段に与える。QOS設定手段は出力データ（該暗号情報を含む所定の情報）に所定の位置かつ／または形式で該QOSを設定・出力する。

【0025】次に、受信側に対する本実施形態を図4を参照にして説明する。

【0026】受信側では、第1の実施形態に示した手段による通信を受けた場合を考える。図4において、QOS分析手段は入力データを分解して、予め定められた情報の位置や識別信号等の形式から暗号情報と階層情報を分解して復号手段に送る。復号手段において制御手段はその階層情報が鍵管理手段に管理されている階層の情報であれば鍵管理手段からその鍵を検索して復号処理手段に入力し、その暗号情報を復号する。さらに、その復号結果が鍵として用いられる階層の情報であれば、その復号結果を鍵記憶手段に一時的に保持させる。また、制御手段はその階層情報が鍵管理手段で管理されていない階層の情報の場合は、保持された復号結果の中からその階層の鍵となる情報を検索してそれを鍵として復号処理手段に入力し、暗号情報を復号し出力させる。ただし、前記の復号結果そもとに演算手段によって鍵を生成する場合もある。よって、QOS分析手段はCPU、DSP等の処理手段やRAM等の記憶手段の組合せで実現でき、復号処理手段は第1の実施形態の暗号処理手段に対応する公知の復号処理手段、鍵管理手段は第1の実施形態と同様の手段、制御手段もCPU、DSP等の処理手段によって実現でき、演算手段もまたCPU、DSP等によって容易に実現できることは明らかである。

【0027】以上は、暗号化及び復号について説明したが、認証が含まれている場合は暗号を署名、復号を検証と置き換えて処理すれば、認証通信に対しても同様の手段によって鍵の重要度に応じた通信が可能であることは明らかである。また、送信と受信を兼ねる装置の場合、

図3、4の構成要素は同様であるので図3，4の手段を合成させた手段（プログラム）を用いることも容易である。

【0028】<第3の実施形態>第1、第2の実施形態においてはコネクション型、コネクションレス型の通信において情報の重要度に応じた通信を実現する手段を各々示した。本実施形態においては第1、第2の実施形態を含む情報の重要度に応じた通信を実現する通信システムについて図5を参照に説明する。

【0029】ここでは一例として第1の実施形態における手段は図5の送信者端末、かつ／または受信者端末に各々内蔵されているとし、図6の階層において階層数K＝2，即ちマスタ鍵とワーク鍵の場合のみを考える。また、コネクション型の通信で、鍵とデータに関する暗号・認証処理は以下に示すＩＤ－ｂａｓｅｄ鍵共有方式によって行われる場合を考える。

【0030】［ＩＤ－ｂａｓｅｄ鍵共有方式］鍵配送手段の管理を行うセンタが存在しており、各エンティティの名前や電話番号などの識別し（ＩＤ）をセンタが受け取り、センタ固有の秘密アルゴリズムを用いて、そのＩＤに対応する秘密鍵を生成して各エンティティに送り、各エンティティはその秘密鍵と通信相手の公開されているＩＤから共有すべき暗号鍵を計算して求める方式である。この方式は、ＩＤ－ｂａｓｅｄ鍵共有方式と呼ばれ、通信相手の確認と鍵の共有が同時に行える。

【0031】この方式は大きく分けて暗号通信に先立つ呼び通信を必要とする方式としない方式に分類される。予備通信を必要とする方式は通信文のみを暗号化して送る電子メールのような使用ができないが、予備通信を必要としない方式は電子メール的な使用ができ、利用範囲が広い。しかし、予備通信を必要としない方式は多くのエンティティが結託した場合、センタの秘密が露呈するという問題がある。予備通信を必要とする方式としては岡本（栄）の鍵配送方式が良く知られており、予備通信を必要としない方式としては松本・今井の鍵配送方式がよく知られている（詳細は辻井，笠原著「暗号と情報セキュリティ」昭晃堂，１９９０．の第４章参照）。以下に、予備通信を必要とする方式の代表的として岡本（栄）の鍵配送方式を示す。

【0032】岡本（栄）の鍵配送方式：

１）センタは一方向性関数として公開鍵暗号方式の１つであるＲＳＡ暗号を公開する。即ち、２つの素数ｐ，ｑ，及び復号鍵ｄを秘密に持ち、ｎ＝（ｐ・ｑ）、及び暗号鍵ｅを公開する（暗号鍵ｅと復号鍵ｄはｅ・ｄ＝１　ｍｏｄ（ｐ－１）・（ｑ－１）の関係をもつ）。さらに、同時に有限体ＧＦ（ｐ）とＧＦ（ｑ）の原始元ｓも公開する。

【0033】２）各ユーザｊはネットワーク加入時に、センタに自分の識別子ＩＤｊを登録し、センタからＳｊ＝ＩＤｊｄ　ｍｏｄ　ｎを計算・送信してもらい、それを秘密に管理する。

【0034】３）ユーザＡとユーザＢは鍵共有を行うとき以下のｉ～ｉｖような通信・計算を行う。

ｉ．ユーザＡは乱数ｋＡを任意に選び、ＣＡ＝ＳＡ・ｇｋＡ　ｍｏｄ　ｎをユーザＢに送る。

ii．ユーザＢは乱数ｋＢを任意に選び、ＣＢ＝ＳＢ・ｇｋＢ　ｍｏｄ　ｎをユーザＡに送る。

iii．ユーザＢはｙ＝（ＣＡｅ／ＩＤＡ）ｋＢ　ｍｏｄ　ｎ（＝ｇｅ・ｋＡ・ｋＢ　ｍｏｄｎ）を計算とする。

iv．ユーザＡはｙ＝（ＣＢｅ／ＩＤＢ）ｋＡ　ｍｏｄ　ｎ（＝ｇｅ・ｋＡ・ｋＢ　ｍｏｄ　ｎ）を計算とする。

【0035】４）ユーザＡ，Ｂともにｙを共有鍵として暗号通信を行う。

【0036】ここで、マスタ鍵は２）におけるＳｊに相当し、ワーク鍵は３）におけるｙに相当する。よって、２）のＳｊは予め各ユーザが有しており、３）の処理・通信が鍵に関する暗号・認証通信であり、４）がデータに関する暗号通信に相当する。また、ユーザＡは図５の送信者、ユーザＢは受信者に相当する。以下、図５の各端末は第１の実施形態に示す手段の他に、公知のＩＤ－ｂａｓｅｄ鍵共有手段を有しているとする（通常、前述のＳｊは該ＩＤ－ｂａｓｅｄ鍵共有手段によって管理されている）。

【0037】先ず、ユーザＡはユーザＢと暗号・認証通信を行う時、先ずＫ＝２として第１の実施形態を用いてネットワークとＱＯＳの交渉を行い、ユーザＢとの間に高品位のＱＯＳをもつコネクションを開設する。コネクション開設後、ユーザＡはユーザＢとの間で公知のＩＤ－ｂａｓｅｄ鍵共有手段を用いて、３）の処理・通信を行い、互いにワーク鍵ｙを共有し、コネクションを一旦終了する。その後、Ｋ＝１として再びネットワークとＱＯＳの交渉を行い、ユーザＢとの間にＫ＝２の場合以下の品位のＱＯＳをもつコネクションを開設する。このコネクションを用いて、ユーザＢとの間でワーク鍵ｙによる暗号通信を実現する。

【0038】次に、コネクションレス型の通信で、マスタ鍵は送信者と受信者で予め共有され、各々の鍵管理手段に格納されており、ワーク鍵は送信者の乱数生成手段で生成される乱数をそのまま用いる場合を考える。この場合、図５の端末は第２の実施形態を含む。

【0039】送信者がデータをワーク鍵で暗号化して受信者に送るとき、先ず送信者は受信者と共有しているマスタ鍵を鍵管理手段から検索し、それによって乱数生成手段の出力であるワーク鍵を暗号化してその階層情報と共にＰＤＵを構成し、ＱＯＳ記憶手段からその階層に対応する高品位のＱＯＳを付けてＡＴＭセル化して受信者に送る。さらに、送信者はその乱数をワーク鍵としてデータを暗号化してその階層情報とともにＰＤＵを構成し、ＱＯＳ記憶手段からその階層に対応する前記のＱＯＳ以下の品位のＱＯＳを付けて同様にＡＴＭセル化して

受信者に送る。

【0040】受信者はセルを合成したPDUから暗号情報、階層情報、送信者、暗号化番号、暗号化の有無等を特定する。ただし、暗号化番号とはワーク鍵とその鍵で暗号化したデータを結び付けるために用いる情報である。よって、受信者は暗号化の有無、及び階層情報等から情報がマスタ鍵によって暗号化されている等を判断し、その場合送信者情報から共有しているマスタ鍵を検索する。さらに、それを鍵として暗号情報を復号し、それをワーク鍵をして暗号化番号と共に鍵記憶手段に保持する。そのPDUが下位の階層に属する場合、暗号化番号が一致するワーク鍵を鍵記憶手段から検索しそれを鍵として暗号情報を復号し、送信者から送られたデータを入手する。

【0041】以上のように、図5の通信システムは種々の鍵とデータに関する通信に適用できることがわかる。

【0042】以上は、簡単のための例であるが、第1、第2の実施形態が外付けである場合、図6が多階層である場合、岡本（栄）のID-based鍵共有法以外の鍵共有法の場合、コネクション型の通信とコネクション型の通信が混在する場合等の各々に対しても同様の通信システムが実現できることは明らかである。また、図5の1つの端末を鍵に関するセンタ局として、送信者と受信者、及びセンタで図4のような階層構造をもつ暗号・認証通信を実現する場合にも、本実施形態が有効であることは明らかである。

【0043】<その他の実施形態>前記の実施形態では情報の重要度に応じた通信を実現するためにQOSを用いたが、通信の品位を実現する手段としてはQOSに限定されず他の実現手段も本発明は含む。その実施形態においては図1～図4のQOSに関する部分をその実現手段に置き換えることによって容易に実現できることは明らかである。

【0044】なお、本発明は、上記処理を実現するための装置と通信端末が分離されていても、1つの機器からなる装置に適用してもよい。

【0045】また、本発明の目的は、前述した各実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUやMPU）が記憶媒体に格納されたプログラムコードを読出し実行することによっても、達成されることは言うまでもない。

【0046】この場合、記憶媒体から読出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【0047】プログラムコードを供給するための記憶媒体としては、例えば、フロッピディスク，ハードディスク，光ディスク，光磁気ディスク，CD-ROM，CD-R，磁気テープ，不揮発性のメモリカード，ROMなどを用いることができる。

【0048】また、コンピュータが読出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているOS（オペレーティングシステム）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0049】さらに、記憶媒体から読出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書込まれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【0050】

【発明の効果】以上説明したように本発明によれば、情報の重要度に応じた通信を実現できる。特に、暗号化における鍵の階層に対応した通信品位を有する通信が実現できるようになる。

【0051】

【図面の簡単な説明】

【図1】実施形態に対する処理手順を示すフローチャートである。

【図2】実施形態における処理構成の概念図である。

【図3】第2の実施形態における送信側の構成概念図を示す図である。

【図4】第2の実施形態における受信側の構成概念図を示す図である。

【図5】第3の実施形態における通信システムの構成を示す図である。

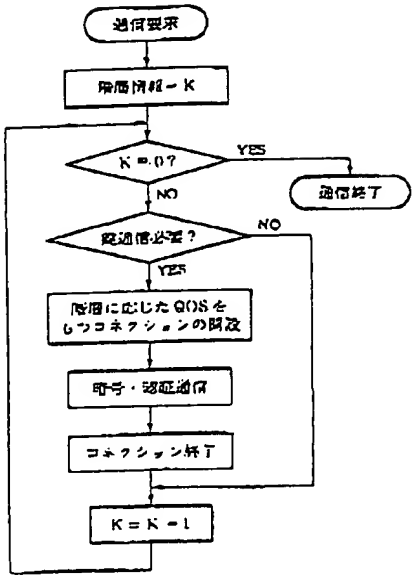
【図6】階層暗号化の概念図である。

【図7】実施形態におけるプロトコルの階層を示す図である。

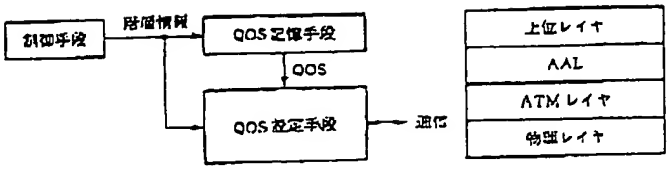
【図8】第2の実施形態におけるコネクションレス型のプロトコルの構成の一例を示す図である。

【図9】第2の実施形態におけるPDUフォーマットを示す図である。

【図1】

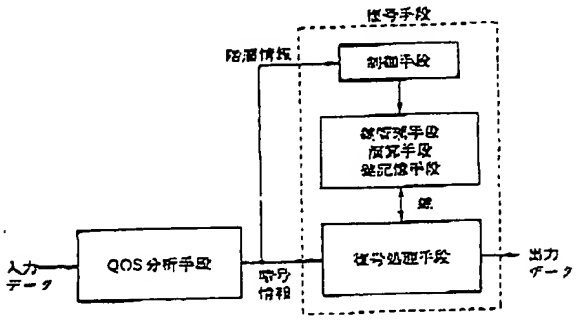


【図2】

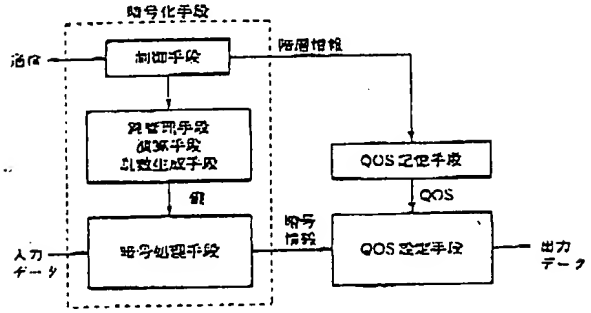


【図7】

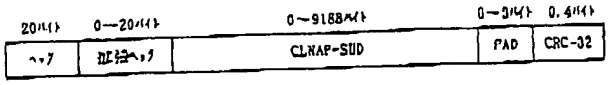
【図4】



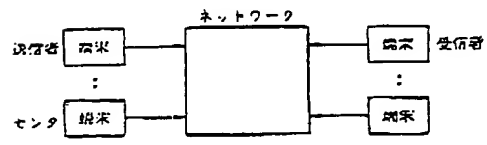
【図3】



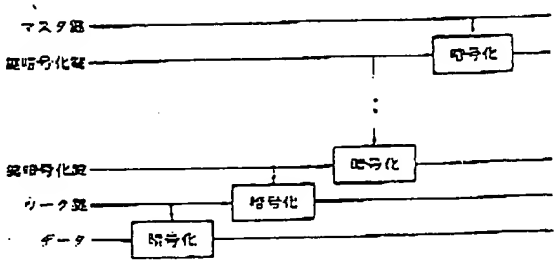
【図9】



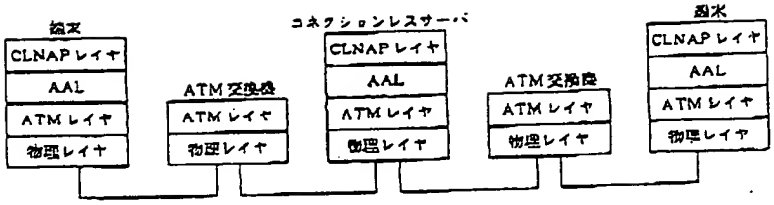
【図5】



【図6】



【図8】


端末
CLNAPレイヤ
AAL
ATMレイヤ
物理レイヤ
ATM交換機
ATMレイヤ
物理レイヤ
コネクションレスサーバ
CLNAPレイヤ
AAL
ATMレイヤ
物理レイヤ
ATM交換機
ATMレイヤ
物理レイヤ
端末
CLNAPレイヤ
AAL
ATMレイヤ
物理レイヤ

The Patent Office
PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS

INVESTOR IN PEOPLE

NDS Limited
% Reginald W Barker & Co.
Clifford's Inn
Fetter Lane
LONDON
EC4A 1BZ

The Patent Office
Patents Directorate

Concept House
Cardiff Road, Newport
South Wales NP10 8QQ

Examiner: 01633 814905
†**E-mail:** Stephen.Brown@patent.gov.uk
Switchboard: 01633 814000
Fax: 01633 814444
Minicom: 08459 222250
DX 722540/41 Cleppa Park 3
http://www.patent.gov.uk

Your Reference: P00/210
Application No: GB 0028501.5

16 August 2001

Dear Sirs

Patents Act 1977: Search Report under Section 17(5)

I enclose two copies of my search report and two copies of the citation.

Publication

I estimate that, provided you have met all formal requirements, preparations for publication of your application will be completed soon after **18 September 2001**. You will then receive a letter informing you of completion and telling you the publication number and date of publication.

Amendment/withdrawal

If you wish to file amended claims for inclusion with the published application, or to withdraw the application to prevent publication, you must do so before the preparations for publication are completed. **No reminder will be issued.** If you write to the Office less than 3 weeks before the above completion date, please mark your letter prominently: **"URGENT - PUBLICATION IMMINENT".**

Yours faithfully

Stephen Brown
Examiner

---

†**Use of E-mail:** Please note that e-mail should be used for correspondence only.

The Patent Office
PATENTS • DESIGNS • COPYRIGHT • TRADE MARKS
INVESTOR IN PEOPLE

Application No: GB 0028501.5
Claims searched: 1-22

Examiner: Stephen Brown
Date of search: 15 August 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): H4P (PDCSX, PPEB)

Int Cl (Ed.7): H04L: 9/00, 9/14.

Other: Online: WPI, EPODOC. JAPIO.

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X	JP 10 009 3547 A (Canon) See especially the abstract.	1-4 & 9-17

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.